ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

DOI: 10.52363/2414-5866-2026-1-33
УДК 351:355.02:005.334

***Абражевич Марина**, аспірантка кафедри публічного управління та адміністрування Університету Григорія Сковороди в Переяславі*
ORCID: 0009-0003-3571-3588

***Abrazhevych Maryna**, Postgraduate student at the Department of Public Management and Administration of the Hrigoriy Skovoroda University in Pereyaslav*

СУЧАСНІ ІНСТРУМЕНТИ РЕАЛІЗАЦІЇ РИЗИК-МЕНЕДЖМЕНТУ У СИСТЕМІ БЕЗПЕКИ ТА ОБОРОНИ

MODERN TOOLS FOR IMPLEMENTING RISK MANAGEMENT IN THE SECURITY AND DEFENSE SYSTEM

У статті здійснено системний аналіз та обґрунтування сучасних інструментів реалізації ризик-менеджменту у системі безпеки та оборони. Сучасні інструменти реалізації ризик-менеджменту у системі безпеки та оборони формують якісно нову парадигму управління, що базується на проактивності, системності та технологічній інтегрованості. Їх розвиток зумовлений ускладненням безпекового середовища, зростанням кількості гібридних загроз та підвищенням ролі інформаційних і кібернетичних чинників у забезпеченні національної безпеки. У цих умовах традиційні підходи до управління ризиками, орієнтовані на реагування постфактум, поступаються місцем інноваційним моделям, які забезпечують раннє виявлення, прогнозування та попередження загроз.

Впровадження цифрових технологій, аналітики великих даних, штучного інтелекту та машинного навчання суттєво підвищує ефективність оцінювання ризиків і прийняття управлінських рішень. Водночас концепція безперервного управління загрозами (CTEM) забезпечує динамічний моніторинг і своєчасне реагування на зміни у безпековому середовищі, що є критично важливим в умовах високої швидкості розвитку сучасних загроз. Застосування сценарного аналізу та симуляційного моделювання дозволяє формувати науково

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

обґрунтовані прогнози розвитку кризових ситуацій і визначати оптимальні стратегії реагування, тоді як використання спеціалізованих рамок кібер- та ШІ-ризиків сприяє систематизації знань про загрози та переходу до проактивного управління ними.

Комплексне поєднання зазначених інструментів забезпечує інтеграцію ризик-менеджменту у стратегічне, оперативне та тактичне управління сектором безпеки та оборони. Це сприяє підвищенню рівня ситуаційної обізнаності, ефективності міжвідомчої взаємодії, оптимізації використання ресурсів та зміцненню стійкості системи до внутрішніх і зовнішніх викликів. У результаті формується адаптивна, гнучка та інтелектуально керована система забезпечення безпеки, здатна ефективно функціонувати в умовах невизначеності та швидких змін.

Ключові слова: *публічне управління, ризик-менеджмент, ризики, системи оборони, архітектура ризик-менеджменту, національна безпека, інструменти реалізації ризик-менеджменту.*

The article provides a systemic analysis and substantiation of modern tools for implementing risk management in the security and defense system. Contemporary risk management tools in this domain are shaping a fundamentally new governance paradigm based on proactivity, systemic coherence, and technological integration. Their development is driven by the increasing complexity of the security environment, the growing number of hybrid threats, and the rising importance of informational and cyber factors in ensuring national security. Under these conditions, traditional risk management approaches focused on ex post response are being replaced by innovative models that enable early detection, forecasting, and prevention of threats.

The implementation of digital technologies, big data analytics, artificial intelligence, and machine learning significantly enhances the effectiveness of risk assessment and decision-making processes. At the same time, the concept of Continuous Threat Exposure Management (CTEM) ensures dynamic monitoring and timely response to changes in the security environment, which is critically important given the rapid evolution of modern threats. The application of scenario analysis and simulation modeling makes it possible to develop scientifically grounded forecasts of crisis situations and to determine optimal response strategies, while the use of specialized cyber and AI risk frameworks contributes to the systematization of knowledge about threats and facilitates the transition to proactive risk management.

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

The integrated use of these tools ensures the incorporation of risk management into strategic, operational, and tactical levels of governance within the security and defense sector. This enhances situational awareness, improves interagency coordination, optimizes resource allocation, and strengthens the resilience of the system to both internal and external challenges. As a result, an adaptive, flexible, and intelligently managed security system is formed, capable of functioning effectively under conditions of uncertainty and rapid change.

Keywords: *public administration, risk management, risks, defense systems, risk management architecture, national security, risk management implementation tools.*

Постановка проблеми. Сучасні інструменти реалізації ризик-менеджменту у системі безпеки та оборони формуються під впливом радикальної трансформації глобального безпекового середовища, що характеризується зростанням гібридних загроз, ескалацією збройних конфліктів, поширенням кібернетичних атак, інформаційно-психологічних операцій та посиленням транскордонної організованої злочинності. У таких умовах традиційні моделі реагування на загрози демонструють обмежену ефективність, оскільки вони орієнтовані переважно на постфактум-реагування, тоді як сучасні виклики потребують превентивного, сценарного та проактивного управління ризиками. Це зумовлює необхідність переосмислення ролі ризик-менеджменту як ключового елементу стратегічного управління у секторі безпеки та оборони.

Ризик-менеджмент у сфері безпеки та оборони виступає інтегрованою системою ідентифікації, аналізу, оцінювання та мінімізації ризиків, що впливають на національну безпеку та обороноздатність держави. Його розвиток пов’язаний із переходом від фрагментарних підходів до комплексних моделей управління ризиками, які базуються на системному аналізі, багатофакторному моделюванні та використанні цифрових технологій обробки великих даних. У цьому контексті значення набувають інструменти прогнозної аналітики, ситуаційного моделювання, систем раннього попередження, а також технології штучного інтелекту, що забезпечують підвищення точності оцінювання загроз і швидкості прийняття управлінських рішень.

Особливого значення набуває інституціоналізація ризик-орієнтованого підходу в системі публічного управління сектором безпеки та оборони, що передбачає інтеграцію ризик-менеджменту у процес стратегічного планування, оборонного менеджменту та кризового

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

реагування. Це відповідає сучасним міжнародним стандартам управління ризиками, зокрема підходам, закріпленим у практиках НАТО та Європейського Союзу, де акцент робиться на стійкості системи, міжвідомчій координації та адаптивності управлінських структур.

Крім того, посилення складності та взаємозалежності загроз обумовлює необхідність розвитку міжсекторальної взаємодії, що включає координацію між військовими, правоохоронними, розвідувальними та цивільними інституціями. У таких умовах сучасні інструменти ризик-менеджменту виступають не лише технічними засобами аналізу, а й інституційними механізмами забезпечення узгодженості управлінських рішень. Це дозволяє підвищити рівень стратегічної передбачуваності, мінімізувати невизначеність та забезпечити ефективне використання ресурсів сектору безпеки та оборони.

Зростання динаміки та багатовимірності загроз, необхідність імплементації міжнародних стандартів управління ризиками, а також потреба у цифровій трансформації управлінських процесів формують стійкий запит на поглиблене дослідження та впровадження сучасних інструментів ризик-менеджменту як системоутворюючого елемента забезпечення національної безпеки та оборони.

Аналіз останніх досліджень і публікацій. Сучасні наукові дослідження у сфері ризик-менеджменту в системі публічного управління обороною свідчать про те, що ця проблематика перебуває на етапі активного становлення, однак характеризується певною фрагментарністю та недостатнім рівнем концептуальної систематизації. Так, А. Лоїшин, І. Ткач, О. Угринович, Д. Окіпняк та М. Потетюєва здійснюють аналіз організаційно-функціональних засад управління ризиками в оборонному секторі, зокрема в контексті діяльності Збройних Сил України. Автори акцентують увагу на прикладних аспектах ідентифікації загроз, ролі внутрішнього контролю як інструменту зниження невизначеності, а також на значенні професійних компетентностей суб’єктів управління ризиками в оборонних структурах. Водночас ці дослідження переважно зосереджуються на операційному рівні ризик-менеджменту, що обмежує можливість формування цілісної теоретико-методологічної моделі.

У наукових напрацюваннях О. Руснака розкриваються концептуальні та методологічні основи ризик-менеджменту в системі публічного управління, включно з оборонною сферою. Дослідник підкреслює системоутворюючу роль міжнародних стандартів, насамперед ISO 31000:2018, як базового нормативно-методологічного фундаменту для формування інтегрованих систем управління ризиками у державному

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

секторі. К. Бугайчук у своїх дослідженнях зосереджується на адміністративно-правових аспектах впровадження ризик-орієнтованого підходу в діяльність органів сектору безпеки й оборони. У роботах Д. Ярмусь досліджується адаптація моделей ризик-менеджменту до умов воєнного стану, що має особливу практичну значущість для сучасної України.

Цілі дослідження є системний аналіз сучасних інструментів реалізації ризик-менеджменту у системі безпеки та оборони.

Виклад основного матеріалу. Сучасні інструменти реалізації ризик-менеджменту у системі безпеки та оборони формуються в умовах принципової трансформації глобального безпекового середовища, яке характеризується високим рівнем невизначеності, динамічністю та багатовимірністю загроз. До ключових детермінант такої трансформації належать гібридизація конфліктів, зростання інтенсивності кібернетичних атак, активне застосування інформаційно-психологічних операцій, розвиток автономних систем озброєння, а також посилення взаємозв’язку між військовими, технологічними та соціально-економічними ризиками. У цих умовах ризик-менеджмент у сфері безпеки та оборони набуває характеру не лише допоміжної управлінської функції, а й системоутворюючого механізму забезпечення стійкості держави та її обороноздатності.

У сучасній науковій доктрині ризик-менеджмент у безпековій сфері розглядається як безперервний процес ідентифікації, аналізу, оцінювання, моніторингу та мінімізації ризиків, інтегрований у цикл стратегічного та оперативного управління. Відповідно до підходів, закріплених у міжнародних стандартах управління ризиками, зокрема Стандарті управління ризиками NIST [1], ризик-орієнтоване управління передбачає інтеграцію безпекових процедур у життєвий цикл системи, включаючи планування, реалізацію, оцінювання та вдосконалення заходів безпеки, що забезпечує системність і безперервність управління загрозами. Подібні принципи також відображені у Стандарті кібербезпеки NIST, який акцентує увагу на функціях ідентифікації, захисту, виявлення, реагування та відновлення як базових елементах ризик-орієнтованого підходу [2].

Першим сучасним інструментом реалізації ризик-менеджменту у секторі безпеки та оборони є цифрові технології та аналітичні платформи, що ґрунтуються на використанні великих даних, методів машинного навчання та технологій штучного інтелекту. Їх інтеграція у систему управління безпекою забезпечує перехід до моделі «управління на основі даних», у межах якої прийняття управлінських рішень базується на

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

комплексному аналізі значних масивів інформації. Це дозволяє підвищити точність оцінювання ризиків і забезпечити їх динамічне прогнозування з урахуванням змін у безпековому середовищі [3].

Використання технологій великих даних забезпечує можливість обробки даних із різних джерел, включаючи розвідувальні дані, кіберінциденти, сенсорні системи та відкриті інформаційні ресурси. Це створює передумови для формування інтегрованих систем ситуаційної обізнаності, здатних здійснювати оцінювання загроз у режимі реального часу. Як зазначається у дослідженнях, ефективність таких систем визначається характеристиками обсягу, швидкості та різноманітності даних [3].

Машинне навчання та штучний інтелект забезпечують перехід до прогнозних моделей управління ризиками, що дозволяють виявляти приховані закономірності у даних і формувати сценарії розвитку загроз. Алгоритми машинного навчання використовуються для автоматизованого виявлення аномалій у поведінці інформаційних систем, що є критично важливим у контексті гібридних загроз та кіберконфліктів [4]. Це дозволяє здійснювати раннє попередження про потенційні інциденти та зменшувати рівень невизначеності у процесі прийняття рішень.

Особливого значення набуває застосування штучного інтелекту у сфері кібербезпеки, де він використовується для виявлення складних багатовекторних атак у режимі реального часу. Відповідно до підходів Національного інституту стандартів і технологій, інтеграція ШІ у системи кіберзахисту дозволяє автоматизувати процеси моніторингу, виявлення та реагування на кіберзагрози, що суттєво скорочує часові затримки між виявленням інциденту та його нейтралізацією [1].

Застосування штучного інтелекту також дозволяє автоматизувати процеси аналізу логів, ідентифікації вразливостей та пріоритизації ризиків. Це особливо важливо в умовах перевантаженості інформаційних систем та обмеженості людських ресурсів у сфері безпеки. За даними досліджень IBM, використання ШІ у кібербезпеці дозволяє суттєво скоротити час виявлення та реагування на інциденти, підвищуючи загальну ефективність системи захисту [5].

Другим важливим сучасним інструментом реалізації ризик-менеджменту у секторі безпеки та оборони є впровадження концепції безперервного моніторингу та управління загрозами, зокрема підходу «безперервного управління загрозами» (далі – CTEM), який передбачає систематичне, циклічне та безперервне виявлення, оцінювання, пріоритизацію та усунення вразливостей у режимі реального часу [6].